

THE CITIZEN

Vol. 35, No. 2

U.S. Army Garrison Stuttgart

January 31, 2006

Stuttgart, Oberammergau and Garmisch, Germany

—Special Edition: Force Protection—

From downrange to the homefront,
safety & security are everybody's business



Petty Officer 1st Class Alan D. Monyelle (Army News Service)

Spc. Wendell Guillermo of the 82nd Airborne Division provides security in Tal Afar, Iraq. Though force protection is obviously a priority downrange, implementing consistent safety and security measures at home, in the office and when on vacation is also essential.

INSIDE THIS EDITION

- Antiterrorism training for all
- Force protection facts
- Keeping our installations safe
- Emergency contact information
- Preventing identity theft
- Staying safe when travelling
- Keeping children safe online
- Talking to your kids about safety
- Office security tips & expectations
- Protecting the computer network
- Preparing to fight the flu
- And much more

Force protection demands constant vigilance

Community members form front line of defense against terror

By Col. Thomas Griffith
Commentary

Longbows, airplanes and truck bombs. Do these things have anything in common? While at first glance they seem totally unrelated, each of them signaled a change in warfare.

In the 13th century an archer with a longbow could fire 10 arrows a minute, each one capable of slicing through chain mail armor, and brought about an end to the knight on horseback. Seven centuries later, the archers were long gone when aircraft arrived over the battlefield and propelled warfare into the vertical dimension, creating a revolution in warfare that continues to reverberate today.

Those who did not adapt to these changes suffered the consequences.

Today, terrorists have changed the face of warfare. As former Central Intelligence Agency Director George Tenet testified, "The threat from terrorism is real, immediate, and evolving."

This does not mean that truck bombs will replace air power. But it does mean that we must adapt to new circumstances.

Worldwide communications via the Internet, cellular phones and other devices, along with modern global travel, give disparate groups the ability to connect and form loose alliances, making it more difficult than ever for law enforcement agencies to detect and stop them.

At the same time, weapons and technology previously reserved for nations can now be used by individuals, magnifying their capacity for death and destruction.

In the past, our force protection efforts against terrorism were intermittent at best. Typically, a great deal of attention would be lavished on the topic shortly after an attack, but interest quickly fell off.

Now and in the future, we have to avoid this haphazard

*You are the number one weapon against this threat.
You must remain alert and aware. You must make force protection
your business. You must be the first line of defense.
After all, your life depends on it.*

approach and maintain a continuous focus on force protection. Terrorism is a worldwide threat and terrorists are searching for the easiest target they can find, wherever it is.

When people say, "it can't happen here," we have to respond, "Yes, it can ... but it will not happen to us."

At the same time, force protection cannot become our overriding goal; otherwise we would do nothing else. A total preoccupation with force protection breeds paralysis and is worse than not paying attention to the new threats.

Instead, force protection has to become an inherent part of our mission and our lives.

Force protection is not just done by security forces. It's an essential part of mission accomplishment, and everyone must treat it that way.

There are ways to beat this threat and accomplish the mission. Part of our adaptation to the new battlefield will be designing new facilities with force protection in mind and investing in technology to produce equipment that can be used to increase security.

But, both now and in the future, the best weapon against a terrorist attack is you. The methods used by terrorists create weaknesses that we can exploit for our own protection.

In most cases, a terrorist does not act without highly ac-

curate information, which means intensive, repeated surveillance conducted over a period of time. This gives you the opportunity to thwart their plans, but you have to be observant enough to recognize what is being done and report it.

Likewise, you have to notice the suspicious package, the individual without the right identification, or the vehicle that seems out of place and then you have to know how to react.

Why you? Because seconds count in these situations, and we can't depend on someone else to do it.

Yes, there will be false alarms, but that's to be expected, part of how we must change and adapt. Better to have a hundred false alarms than to deal with the aftermath of one tragic terrorist incident.

The best weapon we have to defeat the "real, immediate, and evolving" threat of terrorism is vigilance and awareness on your and everyone's part.

You are the number one weapon against this threat. You must remain alert and aware. You must make force protection your business. You must be the first line of defense.

After all, your life depends on it.

This commentary originally appeared online at www.usafe.af.mil.

ON THE STREET

*How do you incorporate force
protection measures into your daily life?*

— Compiled by Antonio Brunetti

THE CITIZEN

Col. Kenneth G. Juergens
U.S. Army Garrison Stuttgart Commander

Public Affairs Officer

Jennifer Sanders
jennifer.sanders@us.army.mil

Editor

Hugh C. McBride
hugh.mcbride@us.army.mil

Assistant Editors

Melanie Casey
melanie.casey@us.army.mil

Christine Castro
christine.castro@us.army.mil

Reporters

Terri Alejandro
terri.alejandro@us.army.mil

Brandon Beach
brandon.a.beach@us.army.mil

Sue Ferrare

susanne.ferrare@us.army.mil

Contact Information

Office Location: Building 3307-W, Kelley Barracks
U.S. Army Address: Unit 30401, APO AE 09107
German Address: Gebäude 3307-W, Kelley Barracks,
Plieningerstrasse, 70567 Stuttgart
Telephone: 421-2046/civ. 0711-729-2046
Fax: 421-2570/civ. 0711-729-2570

This newspaper is an authorized publication for members of the Department of Defense. Contents of The Citizen are not necessarily the official views of, or endorsed by, the U.S. Government or the Department of the Army.

The editorial content of this publication is the responsibility of the U.S. Army Garrison Stuttgart public affairs officer. Private organizations noted in this publication are not part of the Dept. of Defense.

The appearance of advertising in this publication, including inserts or supplements, does not constitute endorsement of the products or services advertised by the U.S. Army.

Everything advertised in this publication shall be made available for purchase, use or patronage without regard to race, color, religion, sex, national origin, age, marital status, physical handicap, political affiliation or any other nonmerit factor of the purchaser, user or patron. If a violation or rejection of this equal opportunity policy by an advertiser is confirmed, the printer shall refuse to print advertising from that source until the violation is corrected.

The Citizen is an offset press publication printed in 6,500 copies every two weeks.

www.stuttgart.army.mil



Kristy Campau

I don't like speaking English with other Americans when I'm downtown.



Corrie Butz

I try not to speak loudly when I'm out and I try to blend in as much as possible.



Wesley Drake

I keep an eye out for suspicious characters — like people pretending they lost their ID to get on post.



Therese Howell

I don't, because I don't know things that potential terrorists would find useful.



Kathy Moner

I'm always aware of what's going on around me — both on- and off-post.



Sherry Ray

Force protection has become second nature for me — for example, like not walking down dark alleys.



Ingrid Amadis

I practice surveillance — I'm aware if someone is watching me, or if a strange package is on my doorstep.



Lisa Davidson

I alter my route when I go home.

Event planning may require force protection coordination

By Christine Castro

So you have reserved the dining hall, booked the caterer, ordered invitations, obtained legal advice – you are on your way to celebrating your next major event, right?

Well, if you have not coordinated with your command force protection office, you may just be in for another task before you sit back and relax.

All official and U.S. sponsored events must have an antiterrorism plan, according to the U.S. Army Garrison Stuttgart Antiterrorism Office, U.S. European Command Operation Order 03-11 and U.S. Army Europe regulation 525-13.

These regulations describe the following criteria and approving authority for each event.

For events conducted on and off installations with 50 to 200 attendees, the USAGS commander is the approving authority.

Events conducted off military installations with 200 or more attendees and events conducted on a military installation with 500 or more attendees need to be approved by the senior mission commander.

Any event with a general officer with a rank of O-9 or 10, or any VIPs in attendance, need also be reviewed by the SMC.

Know the steps, be prepared

Event organizers are to take the following steps no later than 30 days prior to an event with 50 or more individuals in attendance.

- Review the local threat assessment.
- Make a vulnerability assessment and develop AT measures to mitigate the threat.
- Make a risk assessment.
- Prepare an AT plan, operation order or fragmentary order for the event.
- Submit the plan to the garrison AT office for processing.



Hugh McBride

Before your next event, make sure you know what you need to do to ensure maximum protection for all in attendance.

In order to obtain garrison commander or SMC approval, event coordinators need to ensure that they have the following information included with their request.

- Special event organizer's information such as name, rank, e-mail address, unit and contact phone numbers.

- Type of event.
- Date, time and duration of the event.

- Location of event to include street names, city and zip code.

- Number of attendees, to include U.S. and host nation guests with a breakdown of officer, enlisted and civilian personnel.

The list of attendees should also include any host nation representatives with the name of the highest ranking person.

- Mode of transportation to and from the event.

- Identify safe havens along the route to include police stations, hospitals and fire departments.

- Special security requests for VIPs.

- Handicap concerns, if applicable.

- The plan to mitigate known threats or situations that might happen, with a brief paragraph addressing planned actions.

Other critical timelines

If an event requires support by the military police, a request needs to be submitted to the USAGS Provost Marshal's Office no later than 60 days prior to the event.

In order to obtain USAGS commander approval or endorsement for the event, completed AT plan, threat and risk assessments need to be submitted to the USAGS AT Office four weeks prior to the event.

Events requiring approval will be submitted no later than four weeks prior to the event.

The USAGS Antiterrorism Office also encourages personnel to review the USAREUR quarterly travel message which can be obtained from the USAGS Antiterrorism Office.

To contact the USAGS Antiterrorism office call 421-2860/civ. 0711-729-2860.

Family members now required to take antiterrorism training

By Hugh C. McBride

To paraphrase that old commercial about registering for the Selective Service, educating oneself about personal security is not only quick and easy – it's also mandatory.

According to U.S. European Command Operations Order 03-11, family members (ages 14 and above) are now required to complete the Department of Defense's online Antiterrorism Level I training program.

The training, which is available at <https://atlevel1.dtic.mil/at/>, is designed to ensure that all individuals have a heightened awareness of ter-

AT Level I Training is available online at <https://atlevel1.dtic.mil/at/>

rorism and are able to implement personal protective measures into their daily lives.

Training topics include the safe use of public transportation, personal safety when travelling and methods of identifying and reporting security threats.

For more information call the U.S. Army Garrison Stuttgart Antiterrorism Office at 421-2860/civ. 0711-729-2860.

Force protection tips for owners & drivers of privately-owned vehicles

- Never leave personal identification in your vehicle (either on- or off-post).

- Remove all non-required military-related decals from privately owned vehicles (for example, all former post decals, rank, flight wings, jump wings and unit patches).

- Remove U.S. university decals and logos from U.S. sports teams.

- Remove rearview mirror decorations that are associated with U.S. government, organizations or personnel (for example, school graduation tassels and flags from the U.S. states or territories).

- Do not store military uniforms or equipment in vehicles where they can be seen from outside.

- Do not leave copies of orders, mail, newspapers or packages in vehicles where they can be seen from outside the vehicle.

FP ACRONYMS

SNAP

The **Safe Neighborhood Awareness Program** is a USAREUR-wide program similar to stateside "Neighborhood Watch" efforts. For more about SNAP in Stuttgart and Garmisch, see pages 4 and 13.

CAC

The **common access card** (or "smart card") is an integral component of U.S. Army, Europe's installation access control system (see below). The identification card, which is embedded with a computer chip, offers a higher degree of security and accountability than is available with "regular" military ID cards.

FPCON

Force protection conditions are standardized identification and recommended responses to terrorist threats against U.S. personnel and facilities.

Force protection condition levels above "Normal" are:

■ **Alpha:** This condition applies when there is a general threat of possible terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of higher measures.

■ **Bravo:** This condition applies when an increased and more predictable threat of terrorist activity exists.

■ **Charlie:** This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and facilities is imminent.

■ **Delta:** This condition applies in the immediate area where a terrorist attack has occurred or when intelligence indicates that terrorist action against a specific location or person is likely. Normally, this force protection condition is declared as a localized condition.

IACS

Developed in coordination with the Defense Department's Defense Manpower Data Center and 5th Signal Command, U.S. Army, Europe's **Installation Access Control System** is an automated system that employs "smart cards" and handheld digital assistants to move installation access control beyond a reliance on printed ID material.

JSIVA

Begun in the wake of the 1996 terrorist attack on Khobar Towers, Saudi Arabia, **Joint Staff Integrated Vulnerability Assessments** are conducted worldwide to determine force protection vulnerabilities and provide options to assist installation commanders in mitigating or overcoming them.

P.A.U.S.E

Tips publicized to community members to inform them on how to be **Prepared, Alert, Unpredictable, Secure and Exercise caution**. A community force protection awareness campaign focused on getting vital force protection information out to service members, civilian employees and their families.

PCL

Government employees are granted a **Personnel (Security) Clearance** through an administrative determination that the individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

PSQ

A **Personnel Security Questionnaire** and other related information forms are used as part of the investigation process by security personnel in the determination of an individual's access to classified information. An electronic version of the PSQ (EPSQ) is an automated data entry and validation system designed to allow the users (Subjects and Security Officers) quickly and easily enter require data.

Keeping military neighborhoods safe: *Not just law enforcement's responsibility*

By Christine Castro

A child is reported missing an average of every forty seconds in the United States. In other terms, more than 800,000 children go missing in America each year, according to the National Association of Town Watch.

This is one statistic that many families living on an overseas military installation may feel does not apply to them. However, maintaining a strong situational awareness is an essential component of keeping one's family safe wherever one lives.

The Safe Neighborhood Awareness Program is a community based volunteer effort that is designed to improve the security of individuals who live and work on U.S. Army installations in Europe.

Similar to traditional "neighborhood watch" programs, SNAP provides an opportunity for community members to take an active role in protecting the community against terrorists, criminal threats or illegal acts.

One goal of SNAP is to strengthen military communities by encouraging neighbors to get to know one another. The concept is based on the idea that if you know your neighbors and they know you, you have a better chance to identify suspicious activity in your community.

Volunteers on patrol

Following training provided by Stuttgart SNAP Coordinator Ernest Epps, volunteers over the age of 18 – clad in the latest force protection fashion – are on their way to patrolling housing areas for incidents of a suspect nature.

SNAP has also implemented a hands-on training program that allows volunteers to receive their training while they are walking the grounds of a military installation.

SNAP does not promote intervention, and discourages volunteers from taking any unnecessary risks. Instead, the program focuses on improving and sustaining situational awareness and expeditious reporting to the military police.

The timelier and more accurate the information provided to the military police, the better the military police and force protection personnel will be able to assess risks and reduce installation vulnerabilities.

WARNING



NEIGHBORHOOD WATCH

OUR NEIGHBORS ARE WATCHING
OVER ONE ANOTHER'S FAMILY MEMBERS AND
PROPERTY AND THEY HAVE BEEN TRAINED
TO REPORT SUSPICIOUS ACTIVITIES
OR PERSONS IN THE NEIGHBORHOOD
TO THE LOCAL MILITARY POLICE

Make neighborhood safety a SNAP:

Promote a safe and secure environment.

Report abandoned cars, graffiti, vandalism.

Observe surroundings.

Teach others to be aware.

Emphasize good crime prevention habits.

Common sense when off-duty or traveling.

Talk to your neighbors and get to know them.

source: SNAP Web site

tection personnel will be able to assess risks and reduce installation vulnerabilities.

SNAP volunteers say that being a certified SNAP observer is rewarding enough as it is – however, they do enjoy additional benefits.

Volunteers are eligible for prizes ranging from a free meal to free USO tours or a free weekend at the Edelweiss Lodge and Resort in Garmisch.

Everyone's responsibility

You do not have to be a SNAP observer to ensure the safety of you and your family. According to information provided by the SNAP office, the best deterrent to crime is not giving a criminal an opportunity. The U.S. Army Garrison Stuttgart Force Protection office and SNAP regularly publicize tips to help community members keep their families safe.

For more information about SNAP or National Night Out call 430-5560/civ. 0711-680-5560 or 0162-297-5280 in Stuttgart or 440-3558/civ. 08821-750-3558 in Garmisch.

Numbers to know for emergencies in Stuttgart, Garmisch

Military Police: 114

- Stuttgart civ. 0711-680-114
- Garmisch civ. 08821-750-114

* Emergencies only. For non-emergencies call the MP desk - Stuttgart: 430-5262/civ. 0711-680-5262
Garmisch: 440-3801/civ. 08821-750-3801

Ambulance: 116

- Stuttgart civ. 0711-680-116
- Garmisch civ. 08821-750-116

Fire Department: 117

- Stuttgart civ. 0711-680-117
- Garmisch civ. 08821-750-117

Chaplain's Office

- Stuttgart 430-5000/civ. 0711-680-5000
- Garmisch 440-2819/civ. 08821-750-2819

Family Advocacy Program

- Stuttgart 430-7176/civ. 0711-680-7176
- Garmisch 440-2584/civ. 08821-750-2584

Social Work Services

- Stuttgart 431-2627/civ. 07031-15-2627

Garmisch SNAP honored for effort

By Sue Ferarre

Garmisch's Safe Neighborhood Awareness Program has been honored by the U.S. Army for its inaugural National Night Out, an awareness event designed to enhance the community's on-post security.

"The purpose [of National Night Out] is to bring communities together and let neighbors get to know one another," said Garmisch SNAP Coordinator Debbie Manning. "Neighbors who know one another look out for one another," she said.

Among the favorites of the evening's events were a "stranger danger" skit, a military working dogs demonstration and the big hit – an ice cream social, with a make-your-own sundae bar.

"We had child identity kits and a crime scene game," Manning said. "We set up a little crime scene, and community members collected the clues in the crime scene and figured out who was responsible for committing the crime. And then we had that person, once they were identified, arrested and hauled off."

Manning is already working to maintain the programs' momentum, despite her upcoming move.

"Even though I'm leaving my position in March, I've already started the planning for next year's event," she said. "I think it'll be even better than this year."



Drew Benson

A military working dog (and handler) were among the highlights of the Garmisch SNAP program's award-winning National Night Out.

Road condition information in Stuttgart

Receive the most current
road condition information
to help you "Drive to Arrive."

- U.S. Army Garrison Stuttgart Road Condition Hotline – 24-hour updates via a recorded message at 421-2474/civ. 0711-729-2474.

- USAGS Web site – Visit www.stuttgart.army.mil. A weather link is located in the center of the home page. Information is updated around the clock as events warrant.

- AFN Radio – Road condition information broadcast on 102.3 FM every 10 minutes beginning at 5:15 a.m.

- Command Information Channel – Broadcast to all on-post housing in Stuttgart, the CIC slides and text crawl feature weather information and details for locating the latest updates.

Experts advise computer users to stay vigilant against viruses

By Brandon Beach

Spam e-mails have a funny way of just showing up. At first glance, these types of e-mails can look like winning lottery tickets.

The answers to all those midnight prayers wrapped up a simple line such as, "Account Provision of \$45 million."

Forget the fact that the offer comes from an obscure bank in the Republic of Ghana, you suddenly imagine the Caribbean islands. If anything, you reason, it would help with the kids' college tuition.

Before you press that button to start the cyberspace jackpot clinking out your future, it's important to realize that e-mails of this type are not only Internet scams but pose serious threats to the network security of any military community.

"The majority of computer viruses picked up by the Stuttgart footprint come from emails of unknown sources," said Frank Santos, an information assurance network officer with the 52nd Signal Battalion. "If it has multiple attachments or seem suspicious, just delete it."

Santos, along with the entire 52nd team of vigilant Internet watchdogs, work around the clock, along with network safeguarding tools, to make sure that no thread of the enormous volume of daily e-mail traffic takes a wrong turn.

But the real danger of a spam e-mail, if created for the intention of disrupting a personal computer or an entire network, lies in its ability to camouflage itself as an authentic message.

Banks and credit unions are good examples of targets that spammers attempt to spoof in order to obtain personal information, a practice called "phishing."

"We came across one e-mail that asked not only for a person's account number but their ATM password as well."

Another problem with spam emails, whether it's debt re-allocation or the next episode of flying kitty, is the tendency for users to forward them to 10 of their closest friends.

"If you are unsure where it's coming from," said Santos, "never open it or forward it to someone else."

Several red flags - such as the lack of a subject line, obvious misspellings, multiple attachments or

The majority of computer viruses picked up by the Stuttgart footprint come from e-mails of unknown sources.

Frank Santos
52nd Signal Battalion

obscure e-mail addresses - should immediately alert a user.

If you believe you have activated a virus on your computer, the Information Technology Office on Kelley Barracks is another source of assistance and recommends the following steps to safeguard your computer.

"The first thing you should do is immediately disconnect your computer from the network," said computer technician Ron Russell. This can be done by either unplugging the network cable, located in the back of the computer, or disconnecting the power source altogether.

"Then give us a call at the Help desk," said Russell.

Taking work home

Stuttgart community members who choose to burn the midnight oil from home should be aware that computer viruses can easily be transferred from a home computer to a government-licensed machine.

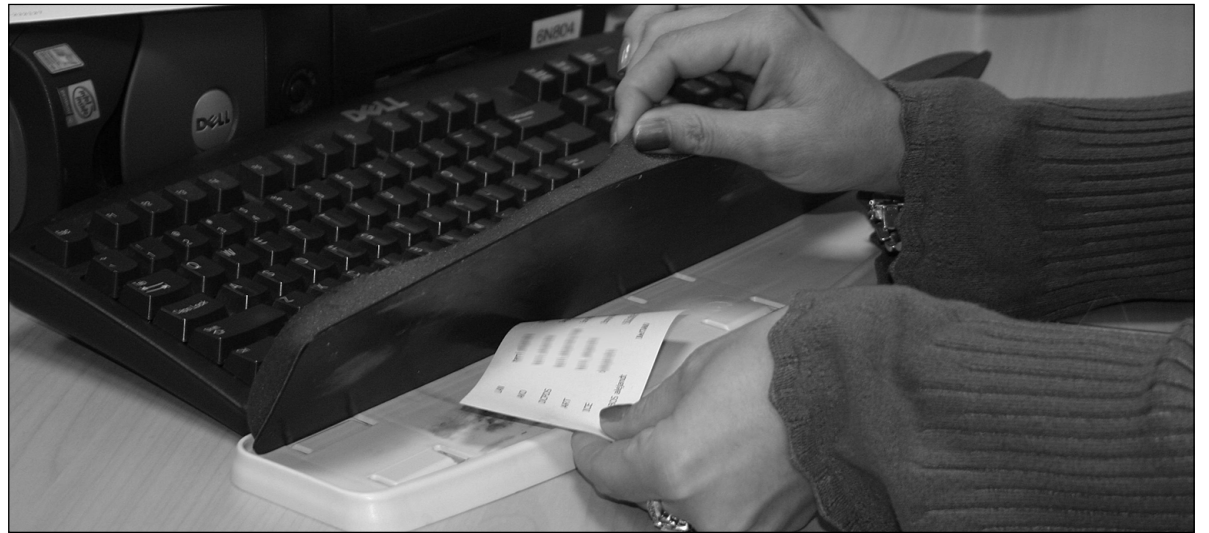
Therefore, Santos notes, it is important that home computers are installed with the latest in anti-virus software to minimize any risk.

Military members, civilian employees and government contractors can download free copies of anti-virus software, firewall protection and anti-spy tools directly from the Army Knowledge Online portal by visiting: <https://www.us.army.mil/suite/login/welcome.html>.

Currently, the portal offers both McAfee and Symantic products.

"If you often work at home, it is important to keep anti-virus up-to-date on your home computer," Santos said.

For computer assistance call the IT Office at 421-2019/civ. 0711-680-2019.



Password security is an integral component of computer network security. Experts advise users to never share their passwords or store them in easily accessible locations, such as beneath a mouse pad or in an unlocked desk drawer.

On government networks, users responsible for keeping system secure

By Hugh C. McBride

Regardless of one's computer expertise - from newbie to techno-wiz - anyone who has access to a military computer shares in the responsibility of keeping the network secure.

Though both software protections and trained professionals work around the clock to keep the network safe, "the user is ultimately responsible for what happens on his or her machine," said Troy Hall, Director of U.S. Army Garrison Stuttgart's Information Technology Support.

Hall said significant technological safeguards are in place to protect the network. However, users must ensure that they don't compromise these efforts - either intentionally or inadvertently.

For example, actions as "innocent" as using a personal digital assistant (such as a PalmPilot) at work or downloading an MP3 music file can hamper the effec-

Computer security tips

- **Never** share your password with anyone.
- Limit Internet access to approved, work-related activities.
- Notify your information management officer **immediately** if your machine malfunctions.
- Do not install software without permission.

tiveness of the network - and are against policy unless done with appropriate approval.

The bottom line, Hall said, is that computer users need to stay aware of local policies and, if in doubt, consult with their information management officer.

"If you notice anything odd about your computer's operation," he said, "you need to notify your IMO immediately."

FORCE PROTECTION ONLINE

The following Web sites are a few of the many force protection resources available in cyberspace:

U.S. Department of State
www.state.gov

Contains information about living and traveling abroad as well as security updates on countries and regions throughout the world.

U.S. Department of Homeland Security
www.dhs.gov

Explains the current color-coded security threat level and precautions; news alerts; an overview of DHS's mission and structure; and other information for citizens, businesses, governments and employees.

U.S. Army, Europe, Automation Training Program
<https://www.uatp.hqusaureur.army.mil>

Features an online computer-user study guide and copy of the USAREUR computer user agreement. Also hosts the test that all must pass before being granted network access.

USAREUR Office of the Provost Marshal
www.hqusaureur.army.mil/opm/opmhome.html

Offers guidance on vehicle and firearms registration, customs, terrorism prevention; provides text of regulations, pertinent links and more.

Defense Threat Reduction Agency
www.dtra.mil

Links to information on combat support; deployed military family support; technology developments relating to weapons of mass destruction; threat control and more.

Fighting the threat from within: Internet access can invite online predators

Federal Bureau of Investigation

Though online computer exploration opens a world of possibilities for children, expanding their horizons and exposing them to different cultures and ways of life, the information superhighway can also be a dangerous place.

Recognizing the risk

Online predators attempt to sexually exploit children through the use of online services and the Internet. Some of these individuals gradually seduce their targets through the use of attention, affection, kindness, and even gifts.

These individuals are often willing to devote considerable amounts of time, money and energy to this process. They listen to and empathize with the problems of children. These individuals attempt to gradually lower children's inhibitions by slowly introducing sexual context and content into their conversations.

Some offenders primarily collect and trade child-pornographic images, while others seek face-to-face meetings with children via online contacts. It is important for parents to understand that children can be indirectly victimized through conversation or "chat," as well as by the transfer of sexually explicit information and material.

Computer-sex offenders may also be evaluating children they come in contact with online for future face-to-face contact and direct victimization. Parents and children should remember that a computer-sex offender can be any age or sex – the person does not have to fit the caricature of a dirty, unkempt, older man wearing a raincoat to be someone who could harm a child.

Children, especially adolescents, may be moving away from the total control of parents and seeking to establish new relationships outside their family.

Sex offenders targeting children will use and exploit these characteristics and needs. Some adolescent children may also be attracted to and lured by online offenders closer to their age who may also be dangerous.

Warning signs

The following signs may indicate that your child might be at risk of being victimized by an online predator:

- Your child spends large amounts of time online, especially at night.

Most children who fall victim to computer-sex offenders spend large amounts of time online, particularly in chat rooms. They may often go online after dinner and on the weekends. Parents should consider monitoring the amount of time their children spend online.

Children online are at the greatest risk during the evening hours. Offenders can be online around the clock, but most work during the day and spend their evenings trying to locate and lure children.

- You find pornography on your child's computer.

Pornography is often used in the sexual victimization of children. Sex offenders often supply their potential victims with pornography as a means of opening sexual discussions and for seduction.

- Your child receives phone calls from people you don't know or is making calls to numbers you don't recognize.

- Your child receives mail, gifts, or packages from someone you don't know.

As part of the seduction process, it is common for offenders to send letters, photographs, and all manner of gifts to their potential victims.

Computer-sex offenders have even sent plane tickets in order for the child to travel across the country to meet them.

Information in this article was prepared from actual investigations involving child victims, as well as investigations where law enforcement officers posed as children.

For more information visit the following Web sites:

- Federal Bureau of Investigation (www.fbi.gov)
- National Center for Missing and Exploited Teens (www.missingkids.org)



www.photos.com

A documented total of 111,530 cases of cyber crimes against children were reported in the U.S. in 2004. Children were victims of crimes including child pornography, child prostitution, child sex tourism, child sexual molestation, enticement of children for sexual acts and unsolicited obscene material sent to a child.

Help your children stay safe online

The Internet can be a dangerous place for children – but strategies do exist to help parents mitigate the threats posed by online predators. The following steps can help families build a solid foundation for safe online experiences:

- **Communicate.** Especially, talk to your child about sexual victimization and potential online danger.

- **Spend time with your children** online. Have them teach you about their favorite online destinations.

- Keep the computer in a **common room** in the house, not in your child's bedroom. It is much more difficult for a computer-sex offender to communicate with a child when the computer screen is visible to a parent or another member of the household.

- Utilize **parental controls** provided by your service provider and blocking software. While electronic chat can be a great way for children to make new friends and discuss various topics of interest, it is also prowled by computer-sex offenders. Use of chat rooms, in particular, should be heavily monitored. While parents should utilize these mechanisms, they should not totally rely on them.

- Always **maintain access** to your child's online account and randomly check his or her e-mail. Be aware that your child could be contacted through the U.S. mail. Be up front with your child about your access and reasons why.

- Find out what **computer safeguards** are utilized by your child's school, the public library, and at the homes of your child's friends. These are all places where your child could encounter an online predator.

- Teach your child the **responsible use** of the resources online. There is much more to the online experience than chat.

Electronic chat can be a great way for children to make new friends and discuss various topics of interest, but it is also prowled by computer-sex offenders

- **Understand** that even if your child was a willing participant in any form of sexual exploitation, he or she is not at fault and is the victim. The offender always bears responsibility for his or her actions.

- **Instruct** your children to always follow the following online safety rules:

- Never arrange a face-to-face meeting with someone you met online.
- Never upload pictures of yourself onto the Internet send photos to people you do not know.
- Never give out identifying information such as your name, home address, school or telephone number.
- Never download files from an unknown source.
- Never respond to messages or bulletin board postings that are suggestive, obscene, belligerent, or harassing.
- Remember: Online information may not be true.

Source: A Parent's Guide to Internet Safety (available online at www.fbi.gov).

Plan ahead to protect your family before, during & after deployment

Brooke Army Medical Center

A family's emotional health can be as important as the physical conditions of each member – and during times of deployment, stresses can transform manageable challenges into seemingly insurmountable obstacles.

Implementing an effective force protection plan for your family doesn't only mean ensuring physical safety.

The following tips (from www.hooah4health.com) are designed to help those who are caring for the child of a deployed service member.

1. Talk as a family before deployment.

Before a deployment, military members are usually preoccupied with many preparatory activities at their military unit, requiring extended hours and an increased workload.

As a result, military members come home tired, perhaps late, and are already reluctant to address painful issues of impending separation. Family members frequently collude in this. It is important to overcome this resistance and make plans with the family as far ahead as possible.

2. Bestow, rather than "dump," responsibilities on remaining family members.

After a parent has been deployed, some children state that everything has changed at home and they now have to do "everything" that the deployed parent used to do.

Discussions before deployment, in which trust and faith in a child's ability to carry out a responsibility are expressed, are valuable times to help the child feel that he or she is important to the family, is important to the deployed parent and can help share a potential burden with the remaining parent.

3. Make plans for the family to continue to progress together, and include the deployed parent in ongoing projects.

It is important that the family not put "life on hold" in anticipation of the return of the deployed parent. This will result in stagnation, loss of direction, and burnout.

Make plans for specific goals to be reached by each of the children and the remaining parent, as well as for family projects to work on together.

Help children design ways to communicate with the deployed parent so that the deployed parent can be part of that progress (for example, by seeing pictures and report cards).

Also, make sure the remaining parent and deployed parent have specific plans on how to communicate.

Include the deployed parent by keeping him or her informed and involved, but do not discuss problems and issues that he or she cannot do anything about.

4. Continue family traditions and develop new ones.

Two stabilizing factors in a family are routines and traditions. Don't stop Friday pizza nights or Saturday outings because the parent has deployed. If anything, become more predictable with your routines.

On the other hand, if the family has not had regular family traditions, now is a good time to start them.

Encourage children to talk about these events and activities during their communication with the deployed parent.

5. Help children understand the finite nature of a deployment by devising developmentally appropriate timelines.

Although the parents may not always know the exact time that the deployment will take place, it can still be helpful to make an estimate and then help children craft a calendar that is illustrated with events to help define the time for them.

Examples to include are holidays, birthdays, special family events and vacations.

Another idea is to create a paper timeline with dates, or a chain made of illustrated paper links, which can be cut cer-



An airman is reunited with his family on Aviano Air Base, Italy, after returning from a deployment in support of Operation Iraqi Freedom. Maintaining family unity before, during and after deployments can be achieved by making – and following – a plan of action.

If one is interested in the well-being of a child, the dictum is always, "Take care of the caretaker."

Unfortunately, because of the many demands upon the remaining parent, it is difficult to make this happen.

Taking care of oneself must be given high priority.

emoniously on a daily basis.

6. To children, no news is worse than bad news.

Studies with children of deployed parents reveal that the children's main preoccupation from day to day is not over the absent parent, but with the remaining parent.

At some level, children are concerned about what is going on with the remaining parent. If that parent becomes cross, self-absorbed or tearful with no explanation, the child's fantasies about that parent's ability to function are worse than reality.

Thus, the remaining parent should be relatively open about sharing concerns and news about the deployed parent.

If the child has an explanation as to why the parent is irritable or preoccupied, he or she is more able to accept the situation.

7. Listen to a child's worries about the deployed parent and answer questions as truthfully as possible.

Follow a child's questions with further questions about what prompted him or her to bring up an issue. Listen carefully first, before trying to dispel what you consider to be false notions on the part of the child.

Explore a child's question to show that you are trying to understand what he or she is worried about, but don't keep pursuing the issue after he or she appears to be satisfied.

Be reassuring about protective measures and training designed to protect the deployed parent, but do not make false assurances about not getting hurt or not dying.

8. Maintain firm routine and discipline in the home.

Under the best of circumstances, maintaining order and routine for children in the home is difficult. It is even more difficult when a parent is suddenly absent.

Children often manifest anxiety about this new separation

– and concerns over the ability of the remaining parent to function – by testing the resolve of the remaining parent, disobeying rules, and flouting routines.

Be proactive and discuss with the child your intent to have very firm routines related to bedtimes, morning routines, room cleanup, chore accountability, and homework. Then follow through with a clear and predictable set of consequences and rewards to keep the program going.

9. Initiate and maintain a close relationship with the school and the child's teacher.

Have a conference with the significant figures in the child's schooling. Make clear to them that the child's parent has been deployed and that there may be an increase in stress at home. Anticipate the first signs of stress in the child.

Signs of vulnerability and stress include deteriorating academic performance, behavioral problems in the classroom, problems in peer relationships, unexplained mood changes, tearfulness or irritability, or worsening of previously existing behavioral problems.

10. As the remaining parent, make sure you take care of yourself.

If one is interested in the well-being of a child, the dictum is always, "Take care of the caretaker."

Unfortunately, because of the many demands upon the remaining parent, it is difficult to make this happen.

Taking care of oneself must be seen as a necessity and given high priority in planning.

Express appreciation to your child when you take the time for yourself, and let him/her know how much better you feel.

This article can be read online at www.hooah4health.com.

Are you sure you're secure?

No one exempt from security responsibilities

By Hugh C. McBride

Wanda Etheridge wants to get inside your head. No, Etheridge isn't part of some nefarious government-sponsored mind control project – but the enemy she's up against can be every bit as dastardly as anything you ever saw on *The X-Files*.

As the security officer for the 6th Area Support Group, Etheridge is responsible for, among other things, ensuring that the members of the Stuttgart military community remain focused on operational security and understand their role in the global effort to ensure national security.

She and her staff give briefings, visit offices and have even posted information online to teach individuals and organizations how to secure their information. But she knows that efforts such as these only go so far.

"We've got to get people in this community to develop a 'security mindset,'" Etheridge said, emphasizing that the difference between knowing and embracing a concept can be the difference between security and disaster. "We have to develop a security foundation that we can build on [with future training sessions, unit briefings and additional education opportunities]."

It's the little things that count

Etheridge and her colleagues in the Army's security business operate under guidance from a number of regulations – including but not limited to AR 530-1 (Operations Security), AR 380-5 (Information Security), AR 380-67 (Personnel Security) and DOD 5200-2-R (DoD Personnel Security).

Obviously, there's more than enough "big picture" guidance out there to occupy the minds and time of all service members and DoD civilians – but Etheridge's primary concern is with the "small" day-to-day tasks that can make or break a security effort.

"Are you shredding all documents before you throw them away?" Etheridge asks. "Are you storing all classified documents in an approved filing cabinet? Are you changing locks and combinations on storage devices in a timely manner? If not, you're committing security violations."

How do you spell 'security'?

During her Security Education and Training briefings, Etheridge uses the acronym SECURITY to help her students remember the core concepts she is trying to get across:

SStorage – Documents must be stored in a manner appropriate for their classification. If you're not sure how to store a document, ask your supervisor – or call Etheridge.

Ensuring "need to know" – Just because your colleague has a secret clearance doesn't mean he or she has a right to see every secret document that comes through your office. Share information only with those who *need* to have access to it. As Etheridge said, "A lot of people don't deal with classified information, but 'for official use only' documents can also do damage in the wrong hands."

Correct classification and markings – A document's security classification requires it to be identified in a particular manner.

Understanding regulations – As everyone who's ever been pulled over after missing a new speed limit sign can tell you, ignorance of the law is no excuse for breaking it. If your job requires you to operate under a set of regulations, it is your responsibility to ensure that you know how to comply.

Reporting violations – Remember that co-worker of yours who makes lots of unnecessary copies, forgets to lock the safe and "accidentally" takes sensitive information home? Reporting these incidents isn't just a good idea – it's also your responsibility as a government employee.

Individual care and caution – OPSEC is more than just following a laundry list of duties and actions – it's exercising personal care and professional caution to protect the assets and information of your organization.

Transmission by authorized means – Even a top-secret clearance doesn't give you the right to paste a classified paragraph into your Hotmail account. In addition to storing information correctly, individuals must also follow proper steps for transmitting (either physically or electronically) that data.

Your responsibility – Finally, though your job description may not include the words "security expert," your association with the Department of Defense mandates that you participate in a vigorous security program. Protecting assets, information and in some cases the lives of fellow employees is a matter of keeping security close to your heart and always on your mind.

The Most Important Person

Remember that old saying about a chain being only as strong as its weakest link? Nowhere is that analogy as applicable as in the world of information security.

Think about it: If 100 people know a secret, achieving a 99-percent "silence success rate" isn't anything to brag about.

Regardless of one's job or access to "important" information, full compliance with the area's security policies and regulations is necessary to guarantee the integrity of operations – and in many cases the lives of the men and women who perform them.

Ensuring that your corner of the world is secure makes it that much harder for our enemies to inflict damage.

For more information about security or related issues call Etheridge at 421-2133/civ. 0711-729-2133 or e-mail etheridge@6asg.army.mil.

Display of Sensitive But Unclassified Information

Having to dig through folder after folder to find the information you're looking for can be such a drag – but posting it where everyone who enters your office can take a peek is a blatant violation of good operational security.

Even if it's not from a "Top Secret" document (which you *do* know not to display, right?), sharing sensitive but unclassified information with the world gives unfriendly agents an additional glimpse into the military environment that you are pledged to protect.

Protection of notes and official documents

You don't have to have a security clearance to have responsibility for protecting information.

Stolen glances through official documents – or even personal notes – can provide information that can damage operations and put lives at risk.

Whenever you leave your workstation – or whenever you have a visitor – be sure that all papers are put away (or at the very least covered up).

Computer Security

Just because you're not an information technology specialist doesn't mean you're exempt from protecting the network.

In fact, being "just a computer user" puts you into the group that poses the greatest risk to our network. No hardware or software can overcome users' failure to follow proper protocol when accessing – or leaving – their government computer accounts.

At the very least, every computer user should take the following steps to protect the network:

- Every time you leave your workstation, lock your computer (CTRL-ALT-DELETE) to prevent unauthorized access.
- Never let anyone else (even a friend) log onto the network with your username and password.
- Don't forward jokes, petitions, chain letters or other unauthorized "spam." This just clogs the network with unnecessary traffic.

Password Protection

Leaving your account password anywhere near your computer (or anywhere where it can be connected to your account) is an invitation to disaster.

Passing the U.S. Army, Europe, computer user test demonstrated your basic understanding of appropriate computer use – but only by following all policies and regulations every day can you ensure that you have not compromised the integrity of the entire network.

Document Disposal (Trash Can vs. Shredder)

Dropping an intact document into the trash doesn't mean you've done your duty to protect the information it contains.

Even non-classified information can help unfriendly agents by providing "one more piece of the puzzle."

According to information provided by the 6th ASG Security Office, "dumpster diving" (or sorting through trash) is one of the main means by which sensitive but unclassified information falls into the wrong hands.

Practicing good operational security includes shredding *all* documents before discarding them. In other words, if you can still read what's on the document, so can the bad guys. Shred, then toss.

Boring photo – or security threat?

It looks like just another office setting – but the "minor" violations illustrated above could be the difference between security and disaster. Remember: If you live or work in the Stuttgart military community, you are responsible for maintaining operational security.

The Most Important Person

Remember that old saying about a chain being only as strong as its weakest link? Nowhere is that analogy as applicable as in the world of information security.

Think about it: If 100 people know a secret, achieving a 99-percent "silence success rate" isn't anything to brag about.

Regardless of one's job or access to "important" information, full compliance with the area's security policies and regulations is necessary to guarantee the integrity of operations – and in many cases the lives of the men and women who perform them.

Ensuring that your corner of the world is secure makes it that much harder for our enemies to inflict damage.

Workplace Security Quiz

*How informed are you about what it takes to keep your organization safe?
[Answers inverted at bottom of quiz.]*

- [TRUE/FALSE] I can allow a trusted co-worker to log onto the network under my username if I make sure to change my password immediately after he or she logs off.
- [TRUE/FALSE] If I use my Army Knowledge Online account, it is safe to send my social security number or other personal data via e-mail.
- If I sign an SF 312 Non-Disclosure Agreement, I am bound by that document for ...
a) 5 years c) the duration of my career
b) 10 years d) life
- [TRUE/FALSE] Refusing to sign an SF 312 will result in the suspension of my access to classified information.
- According to AR 380-67 (Personnel Security Program), if I am granted a top secret clearance I will be reinvestigated every ____ years.
a) 5 years c) 10
b) 7 years d) few
- The classification of a document should be marked on ____ page(s).
a) the first c) the first and last
b) the last d) every
- If you plan to travel to a foreign nation (outside Germany) on **official** business you ____ receive a threat briefing before departing.
a) must c) can
b) should d) oughta
- If you plan to travel to a foreign nation (outside Germany) on **personal** business while on leave you ____ receive a threat briefing before departing.
a) must c) can
b) should d) oughta
- Local OPSEC policy calls for ____ documents to be shredded before being discarded.
a) sensitive c) secret
b) classified d) all
- [TRUE/FALSE] Local national employees are not required to participate in security measures such as those described on these pages.
- [TRUE/FALSE] Using my government computer to access the Internet for personal use is permitted.
- [TRUE/FALSE] When mailing a classified document, I must write or stamp "Classified" clearly on the mailing envelope.

Answers

1-False; 2-False; 3-d; 4-True; 5-a; 6-d; 7-a; 8-a; 9-d; 10-True; 11-True; 12-False
Still have questions? Call the 6th ASG Security Office at 430-2133/civ. 0711-729-2133 or e-mail etheridge@6asg.army.mil.



Maria Higgins

Baseball cap, white tennis shoes, "NYC" sweatshirt – some Americans can shout out their nationality without ever saying a word. Before heading out the door when traveling or living abroad, ensure that you haven't put yourself at undue risk due to your appearance.

Out 'n' about? Blend in for safety

By The Citizen

The current atmosphere of heightened security should not keep American military members and civilians from enjoying the sights in Europe.

For example, attending German fests or fasching events can be fun adventures that introduce Americans to their host country.

However, certain safety precautions should always be taken in order to ensure a safe and pleasant experience.

All individuals should exercise caution and common sense when venturing out. The 6th Area Support Group security office offers the following guidelines:

- Maintain a low profile. Avoid being obnoxious and loud. Your conduct and mannerisms should not attract attention. Keep voices low.

- Don't go out in large groups. Smaller groups are much less likely to be noticed.

- Dress to blend in – not to stand out. Certain types of clothing (for example, cowboy hats, white tennis shoes and baseball caps) may identify you as an American. Try to wear something more typical of what Europeans would wear.

- Be alert to your surroundings. Watch for suspicious people. If you think you are being followed, go to a secure area (the German Polizei always have a station at fests).

Never confront the individual following you, but obtain the best possible description and report it to the police.

Have fun – but stay safe

- Travel in a small group.
- Dress to blend in.
- Conceal military affiliation.
- Be alert for suspicious individuals and situations.
- Supervise children closely.
- Limit alcohol intake.



- If possible, park your vehicle in a secured lot. Otherwise, try to park in a well-lighted area. Parking can be a nightmare if you visit a fest in the evening. It's simpler to take public transportation.

- The possibility of children becoming lost is real. If children are along, watch them closely and choose a meeting point in case someone becomes separated from the group.

Talk to children about what to do in such a situation.

- Don't discuss your military affiliation with strangers.

- Limit alcohol intake. Try not to overindulge, and plan transportation home in advance. Have a designated driver. This is important for those who leave their cars at park-and-ride stations, too.

Criminals target travelers' automobiles, wallets

U.S. Department of State
Bureau of Consular Affairs

In many places frequented by tourists, including areas of southern Europe, victimization of motorists has been refined to an art.

Where it is a problem, U.S. embassies are aware of it and consular officers try to work with local authorities to warn the public about the dangers.

In some locations, these efforts at public awareness have paid off, reducing the frequency of incidents.

Carjackers and thieves operate at gas stations, parking lots, in city traffic and along the highway. Be suspicious of anyone who hails you or tries to get your attention when you are in or near your car.

Criminals use ingenious ploys. They may pose as "good Samaritans," offering help for tires that they claim are flat or that they have made flat. Or they may flag down a motorist, ask for assistance and then steal the rescuer's luggage or car.

Usually they work in groups, with one person carrying on the pretense while the others rob you.

Other criminals get your attention with abuse, either trying to drive you off the road, or causing an "accident" by rear-ending you or creating a "fender bender."

In some urban areas, thieves don't waste time on ploys – they simply smash car windows at traffic lights, grab your valuables or your car and get away.

In cities around the world, "defensive driving" has come to mean more than avoiding auto accidents; it means keeping an eye out for potentially criminal pedestrians, cyclists and

In cities around the world, "defensive driving" has come to mean more than avoiding auto accidents – it means keeping an eye out for criminal activities.

scooter riders.

Both in and out of vehicles, travelers should avoid carrying large amounts of cash.

Also, change travelers' checks only as currency is needed – and make sure to countersign them only in front of the person who will cash them.

Do not flash large amounts of money when paying a bill. Make sure your credit card is returned to you after each transaction.

Deal only with authorized agents when you exchange money, buy airline tickets or purchase souvenirs. Do not change money on the black market.

If your possessions are lost or stolen, report the loss immediately to the local police. (A state-side driver's license, department store credit cards, and other nonessential means of identification should have been kept at home to begin with.) Keep a copy of the police report for insurance claims and as an explanation of your plight. After reporting missing items to the police, report losses or thefts to the following:

- travelers' checks: nearest agent of the issuing company.
- credit cards: the issuing company.
- passports: nearest U.S. embassy or consulate.

Travel safety starts at home: Precautions thwart criminals

U.S. Army Installation Management Agency, Europe Region, Release

Staying alert and taking the following precautions can help ensure safety both at home and on the road:

Before departure

- Do not discuss travel plans in public places; only tell those who need to know the details (for example, one's unit or supervisor).
- Check the U.S. State Department Web site for security information on all countries to be visited or travelled through.
- Ensure that all doors and windows – including those in the garage – are secure.
- Use automatic timers to turn lights, radios and televisions on and off to make it appear as if someone is home.
- Unplug all unnecessary electrical equipment
- Ask a neighbor to keep an eye on the home and remove mail and newspapers.
- Ask a neighbor to draw the curtains in the house at night and open them in the morning.
- Do not hide a spare key; instead leave one with a trusted neighbor.
- Use civilian addresses for tickets and other travel documents.

On the road

- Never leave keys unattended.
- Never leave luggage unattended.
- Never carry packages for other people.
- Do not display military identification, stickers or unit logos.
- Do not leave items of military equipment or clothing visible in the car.
- Conceal military-issued car passes.
- Keep a low profile, and be discreet in revealing NATO and military affiliation.
- Do not flash large sums of money, and do not carry documents, credit cards or unnecessarily large sums of money.
- Carry valuables and belongings in a secure manner.
- Check the underside of unattended vehicles before entering them.
- Avoid secluded areas, poorly lighted streets and alleys.
- Stay away from known "trouble spots."
- Be wary of pickpockets, especially in crowded areas.



Preparing for Pandemic

Threat of avian flu outbreak prompts proactive response among individuals, groups, governments

By Maj. Pamela Cook
U.S. European Command

Officials met in Stuttgart recently to plan for how best to deal with a potential outbreak of avian influenza that could mutate into a pandemic flu.

Conference attendees, including subject matter experts from throughout the region, worked to create a comprehensive plan in coordination with U.S. European Command, host nations, the Department of Defense and other governmental agencies to deal with a possible pandemic caused by the mutation of the H5N1 influenza virus, more commonly known as “bird flu,” that is currently circulating through domestic and wild bird flocks around the world.

“Due to the serious consequences presented by a potential pandemic, and in support of U.S. government worldwide efforts, EUCOM is coordinating with appropriate organizations and governments to ensure that people are protected and informed,” said Air Force Lt. Col. Ron Sanders, the lead project officer for EUCOM’s pandemic influenza response team.

A united effort

The DoD, Department of State, Health and Human Services, World Health Organization and other governments and agencies are preparing for a possible pandemic – a global outbreak of disease – of avian influenza.

These organizations are building on the knowledge and experience from other recent public health crises, including SARS and the 2001 anthrax attacks, to meet the threat of a pandemic outbreak.

EUCOM and its component commands are continuing the planning process to protect their service members, family members and employees while maintaining operational readiness.

Planning ahead

The presence of even a limited number of human cases of avian influenza has raised concerns that a pandemic could occur if the virus develops the ability to spread from human to human.

If such a situation should occur in Europe, the EUCOM plan suggests individuals should be prepared to increase good personal hygiene practices such as hand washing, cough and sneeze etiquette, and care in food preparation. In the event of an epidemic avian

“When the next pandemic strikes, it is likely to touch the lives of every individual, family and community. Our task is to make sure that when this happens, we will be a nation prepared.”

Michael O. Leavitt
U.S. Department of Health & Human Services

influenza outbreak, social distancing, isolation and quarantine procedures may have to be implemented.

Social distancing includes limiting social gatherings and interactions such as attending school, churches, civic clubs and groups, and work activities. Local commanders and health officials will notify personnel of specific procedures on their installations.

Medical response

Some existing antiviral treatments are available to possibly mitigate a pandemic influenza virus. There is currently no vaccination available to counter the virus in its existing form.

Once the bird flu virus has mutated to where it can be passed from human to human, experts estimate that it will take at least six to nine months to develop an effective vaccine. However, the mitigating antiviral medications have proven somewhat successful at blocking the replication of the virus if treatment begins within 24 to 48 hours.

While it is unusual for people to get influenza infections directly from animals, sporadic human infections and outbreaks caused by certain avian influenza viruses are cause for concern.

These sporadic human infections, however, rarely result in sustained transmission among humans. Avian flu currently does not have the ability to be transmitted through human-to-human contact.

In order for the bird flu virus to cause a pandemic, several factors must be present.

According to a town hall meeting on the subject hosted by the American Consulate General in Frankfurt, the most notable factors include the ability for the virus to replicate itself in humans and to be efficiently able to transmit from human to human. There is currently no indication that the virus has changed to a form that could result in a pandemic.

What’s the Difference?

A number of crucial distinctions exist between seasonal flu and pandemic flu.

Seasonal Flu	Pandemic Flu
Outbreaks follow predictable seasonal patterns. Seasonal flu occurs annually, usually in winter, in temperate climates.	Outbreaks occur rarely. In the 20th century, pandemic flu occurred only three times, with the last outbreak in 1968.
Individuals usually have some immunity (which was built up from previous exposure).	No previous exposure means little or no pre-existing immunity is present.
Healthy adults are usually not at risk for serious complications. Increased risk is generally limited to the very young, the elderly, and those with certain underlying health conditions.	Healthy individuals may be at increased risk for serious complications.
Health systems are usually prepared to meet public and patient needs.	Health systems may be overwhelmed.
Vaccine is developed based upon known flu strains and is available for the annual flu season.	Vaccine would likely not be available in the early stages of a pandemic.
Average annual number of flu-related deaths in the United States is 36,000.	The 1918 pandemic caused 500,000 deaths in the U.S. and 40 million deaths worldwide.
Generally has modest impact on society (for example, some school closings, encouragement of affected individuals to stay home from work).	May cause major impact (for example, travel restrictions, cancellations of public events, widespread closures of schools and businesses).

The complete document from which this excerpt was taken can be accessed online at www.pandemicflu.gov/season_or_pandemic.html.

Information, preparation keys to fighting flu

An influenza pandemic is a widespread outbreak of disease that occurs when a new flu virus appears. Pandemics are different from seasonal outbreaks of influenza.

A pandemic may come and go in waves, each of which can last for months at a time. An especially severe pandemic could lead to high levels of illness, death, social disruption and economic loss.

The United States has been working closely with other countries and the World Health Organization to strengthen systems to detect outbreaks of influenza that might cause a pandemic.

Individuals can help limit the spread of the flu. Take common-sense steps to limit the spread of germs. Make good hygiene a habit:

- Wash hands frequently with soap and water.
- Cover your mouth and nose with a tissue when you cough or sneeze.
- Keep raw poultry away from other foods.
- Keep hands, utensils and surfaces clean.
- Use a food thermometer to ensure poultry has been fully cooked.
- Stay at home if you are sick.
- Exercise on a regular basis and get plenty of rest.

The information in this article was compiled from “Pandemic Influenza Planning: A Guide for Individuals and Families,” which is available online at www.pandemicflu.gov.

Influenza information: online resources

The following Web sites are excellent sources of information related to avian influenza as well as a number of other health-related issues.

U.S. Centers for Disease Control
www.cdc.gov

- Click “Avian Flu” on the main page.
- Information includes details about the virus (including how it is spread and prevented) as well as updates on outbreaks around the world.

U.S. Food & Drug Administration
www.fda.gov

- Click “Flu Information” in “Hot Topics” section.
- In addition to flu facts, the site includes updates on vaccine development and fraudulent products.

Pandemic Flu Information Page
www.pandemicflu.gov

- The official U.S. government Web site for information on pandemic flu and avian influenza.
- Information addresses individuals, schools and businesses, governments and more.

U.S. State Department
www.travel.state.gov

- Click “International Travel” on the main page, then “Health Issues.”

Protecting our installations

JSIVA: Stopping terrorists before they strike

By Christine Castro

It took the deaths of nearly 3,000 individuals in the destruction of the World Trade Center's Twin Towers to raise awareness among Americans about the ominous threat facing them and those who fight for peace and democracy throughout the world.

New kind of enemy

Following the 9/11 terror attacks, U.S. President George Bush explained to the American people that the nation was engaged in a struggle against "a new kind of enemy." That enemy, he said, is terrorism.

Until Sept. 11, 2001, this treacherous enemy seemed almost invisible to the majority of the American public.

However, the fight against terrorism did not start on Sept. 11, and the United States armed forces is no stranger to identifying the enemy and protecting the nation against those whose mission is to strip others of their liberties — and their lives.

With each news report of a suicide bombing or a vehicle explosion, the world becomes more familiar with the enemy and its unconventional war tactics.

Security experts believe that this war can no longer be fought entirely by the military as our predecessors have done.

The fight to eradicate terrorism, experts believe, demands educating the American people and empowering them to protect themselves from the threat that may lurk in their own backyards.

Fighting the war at home

Empowering service members and their families is exactly what the U.S. Army Garrison Antiterrorism Office, in cooperation with the Safe Neighborhood Awareness Program and area military police have committed themselves to do through the area's antiterrorism program.

Although the enemy often uses unpredictable tactics and attacks unspecific targets, ordinary individuals can prevent terrorists from having the ability to exploit vulnerabilities.

P.A.U.S.E. for safety

The USAGS Antiterrorism Office regularly releases security information in the form of P.A.U.S.E. (Prepared, Alert, Unpredictable, Se-

The purpose of a JSIVA inspection is to identify effective practices that may be used on installations worldwide.

cure and Exercise caution) tips to help community members limit their opportunities to becoming a terrorist's target.

These P.A.U.S.E. tips are part of the area's force protection awareness campaign.

Another attempt to improve counter-terrorism measures and raise community awareness is the Joint Staff Integrated Vulnerability Assessment, or JSIVA.

Lessons learned

After 19 U.S. service members were killed and 502 were wounded in the bombing of the Khobar Towers in Saudi Arabia in 1996, retired Gen. Wayne A. Downing was appointed by then-Secretary of Defense William Perry to assess the adequacy of force protection on the Arabian Peninsula and the Khobar Towers.

Downing's report concluded that there were serious deficiencies in force protection at the Khobar Towers as well as at other Central Command facilities.

He also recommended implementing force protection improvements worldwide.

Virtually all of Downing's recommendations were adopted by the DoD, and changes were effected to better protect personnel and mission-essential infrastructure.

Following Downing's investigation and subsequent report, standards were established and a process was implemented to regularly assess vulnerabilities on U.S. installations.

Established in 1997, this assessment process is known as JSIVA.

JSIVA teams located in Alexandria, Va. now make up an integral part of the Defense Threat Reduction Agency's combat support directorate.

Six JSIVA teams assess 100 installations each year throughout the services, defense agencies and combatant commands.



On June 25, 1996, a terrorist truck bomb exploded outside the northern perimeter of the U.S. portion of the Khobar Towers housing complex in Dhahran, Saudi Arabia. The explosion, which killed nineteen service members and wounded hundreds of others, prompted the Department of Defense to implement the JSIVA process of assessing installation security.

A JSIVA inspection of USAGS is tentatively scheduled for February 2006.

How JSIVA helps

The purpose of a JSIVA inspection is to provide the installation commander with an assessment of his or her antiterrorism program, recommend any necessary improvements, and finally, to identify effective installation practices that may be used on other installations worldwide.

In preparation for the on-site visit, the team (comprised of six antiterrorism experts) reviews previous assessments to ensure remedial actions were taken.

The team also reviews the installation's plan to ensure its compliance with DoD antiterrorism standards as described in DoD Instruction 2000.16.

JSIVA inspections, to include two appraisals, are typically conducted in two weeks.

Upon completion of the inspection, the team chief will deliver an out-brief to the installation commander and staff.

A comprehensive report of the findings will be generated within 45 days of the completion of the inspection.

Last year, the Department of Homeland Security budgeted approximately 36 billion dollars in order to protect the nation against those who threaten Americans' civil liberties, and who were willing to die for that cause.

However, one of the greatest deterrents against terrorists is the American citizenry.

With public awareness and education of terrorist threats and tactics, Americans are better equipped to protect themselves, their families and their freedom.

Find P.A.U.S.E. tips and information on antiterrorism initiatives see future issues of The Citizen and the Stuttgart Community Post (online at www.stuttgart.army.mil).

For more information about how you can help protect your family and community through SNAP call 430-5560/civ. 0711-680-5560 (in Stuttgart) or 440-3618/civ. 08821-750-3618 (in Garmisch).

U.S. Army Garrison Stuttgart Security and Intelligence Division "Lunch and Lecture" Series

(Lectures will last from 11:30 a.m. to 12:30 p.m.)

- Feb. 22 – E-mail Encryption/Digital Signature: An explanation of what the CAC is and how to use it.
- March 22 – Identity Theft/Privacy Act: Why you must protect personal information.
- April 26 – Processing an Installation Pass Application from Start to Finish: The basics of AE Regulation 190-16.
- May 24 – Safe Management: How to change combinations, complete paperwork, and more.
- June 21 – Security in the Workplace: Security is everyone's business; gain some helpful office tips.

The lectures will be held on Kelley Barracks (Building 3307, Classroom #4)

Feel free to bring a bag lunch. Beverages will be provided.

Register by sending an e-mail containing your name, contact number and unit to wanda.etheridge@us.army.mil or eshe.wyatt@us.army.mil.

For more information call the U.S. Army Garrison Stuttgart Security Office at 421-2824/2133/civ. 0711-729-2824/2133.



Safe Neighborhood Awareness Program

**Help SNAP keep
our installations safe.**

Stuttgart

DSN: 430-5560

CIV: 0711-680-5560

earnest.epps@us.army.mil

Garmisch

DSN: 440-3618

CIV: 08821-750-3618

debbie.l.manning@us.army.mil





Can *you* pass the force protection quiz?

Find out how informed you are on local, national and international issues related to force protection and global security. (Answers, page 15)

Section I: Stuttgart & Garmisch

1. To notify military police of an emergency (via DSN phone) dial:
a) 911 b) 123 c) 114 d) 999

2. In addition to military police troops assigned to U.S. Army Garrison Stuttgart, Soldiers from the _____ also help protect Stuttgart-area installations.
a) 10th Mountain Division c) 5077th Mobile Army Surgical Hospital
b) 554th Military Police Company d) 5th Military Police Brigade

3. Match each insignia below with the organization it symbolizes:
a)  b)  c)  d) 
i. U.S. Army Garrison Stuttgart iii. U.S. Army, Europe
ii. Installation Management Agency iv. U.S. European Command

4. The local program that is similar to a stateside "Neighborhood Watch" is ____.
a) SNAP b) SNARE c) DARE d) UNCLE
5. FP condition(s) (?) is/are designed to be maintained for an extended period of time.
a) Alpha b) Alpha, Bravo c) Alpha, Bravo, Charlie d) Alpha, Bravo, Charlie, Delta

6. Road conditions in military communities are listed (from least to greatest difficulty) as:
a) red, blue, green b) yellow, orange, red c) green, amber, red d) red, white, blue

7. The U.S. Army Garrison Stuttgart Web site can be accessed at:
a) www.6asg.army.mil c) www.army.mil/stuttgart
b) www.usags.mil d) www.stuttgart.army.mil

8. In Stuttgart, American Forces Radio can be found at:
a) 1143 AM/102.3 FM b) 1180 AM/107.7 FM c) 1485 AM/90.3FM d) 999 AM/99.9FM

9. In Garmisch, American Forces Radio can be found at:
a) 1143 AM/102.3 FM b) 1180 AM/107.7 FM c) 1485 AM/90.3 FM d) 999 AM/99.9FM





10. (T/F) Under road condition amber, military vehicles can be driven only from installation to installation in the immediate area.
- Bonus

What does "DPTMS" stand for?

Section II: United States

1. The U.S. Department of Homeland Security is led by Secretary _____.
a) Michael Chertoff b) Condoleeza Rice c) Bernard Kerik d) Tom Ridge

2. In the United States, terror alerts are issued (from least to greatest threat) as:
a) green, blue, yellow, orange, red
b) white, yellow, orange, red, black
c) white, green, blue, red, black
d) ecru, mauve, teal, heather, espresso

3. Match each individual below with his title:
a)  b)  c)  d) 
i. Chairman, Joint Chiefs of Staff iii. Secretary of Homeland Security
ii. Secretary of Defense iv. Chief of Staff, U.S. Army

4. If President Bush and Vice President Cheney are incapacitated, (?) would serve as president.
a) Secretary of Treasury John Snow c) Speaker of the House Dennis Hastert
b) Secretary of Defense Donald Rumsfeld d) Senate Majority Leader Bill Frist

5. Before becoming Secretary of State, Condoleeza Rice served as _____.
a) Deputy Secretary of State b) National Security Advisor c) Director of Homeland Security

6. _____ became the United States's first Director of National Intelligence in April 2005.
a) John Bolton b) John McCain c) John Shalikashvili d) John Negroponte

7. The last president to be a military academy (Army, Navy or Air Force) graduate was _____.
a) George H.W. Bush b) Jimmy Carter c) John F. Kennedy d) Dwight Eisenhower

8. Which U.S. president also served as director of the Central Intelligence Agency?
a) John F. Kennedy b) Ronald Reagan c) Jimmy Carter d) George H.W. Bush

9. (T/F) U.S. troops cannot be sent into battle without a joint resolution from Congress.




10. (T/F) No Marine has ever served as Chairman of the Joint Chiefs of Staff.
- Bonus

Donald Rumsfeld is the oldest man to serve as U.S. secretary of defense. Who is the youngest man to hold this position?

Section III: International

1. The secretary-general of the North Atlantic Treaty Organization is:
a) Kofi Annan b) George Robertson c) Boutros Ghali d) Jap de Hoop Scheffer

2. Travel advisories can be found on the Internet at:
a) www.state.us.gov c) www.traveladvisories.com
b) www.ustravel.gov d) www.dontbeavictim.com

3. Match each individual below with his title:
a)  b)  c)  d) 
i. United Nations Secretary-General iii. Supreme Allied Commander, Europe
ii. NATO Secretary-General iv. U.S. Ambassador to the United Nations

4. Which of the following is not a member of NATO?
a) Spain b) Sweden c) Belgium d) Luxembourg

5. Which of the following is not a member of the European Union?
a) Estonia b) Slovakia c) Slovenia d) Turkey

6. The George C. Marshall Center was founded in response to:
a) an attempted coup in the Soviet Union c) the fall of the Berlin Wall
b) the massacre in Tiananmen Square d) ethnic cleansing in Yugoslavia

7. The five permanent members of the United Nations Security Council are the United States, the United Kingdom, Russia, France and _____.
a) Germany b) Japan c) China d) Italy

8. (?) does not share a border with Iraq
a) Kuwait b) Afghanistan c) Syria d) Iran

9. Hamid Karzi is the elected leader of _____.
a) Iraq b) Iran c) Afghanistan d) Ukraine

10. The president of _____ recently called for the destruction of _____.
a) China, Taiwan b) India, Pakistan c) Iran, Israel d) Venezuela, Nicaragua
- Bonus

What is the English translation of "Al-Qaeda"?

Directions

■ Un-jumble the following 10 words, then find them in the search square.

■ Words in the square are forward, backward, up, down and diagonal.

Colors of the U.S. flag:

1. _ _ _ _
(ERD)
2. _ _ _ _ _
(TEHWI)
3. _ _ _ _ _
(ULEB)

3 types of military in Stuttgart:

4. _ _ _ _ _
(YARM)
5. _ _ _ _ _ _ _
(RAI ORCFE)
6. _ _ _ _ _
(VNYA)

R E D E R E R E E C R O F R I A
S T U T T G A R T D A H P E A H
A J X J A S X V P J B E O J A J
R K O V R N A V Y K R L L I M K
M Q M Q M A U Q T Q M Q I O M W
Y V E A Y P Y V R V Y V C V Y H
L M E P R B G Y M O C U E I L I
A F G E A I A E P S E B E Q U T
B Z P T B O N T P S B K B R X E
B L U E A M A E U M A E A Y A M

- U.S. Army Garrison _____
7. _ _ _ _ _ _ _
(TTTTGSARU)
- 554th Military ____ Company
8. _ _ _ _ _ _ _
(PCLEOI)
- U.S. European Command
9. _ _ _ _ _ _ _
(ECOMU)
- Gen. James Jones is a _____
10. _ _ _ _ _ _ _
(AMRNEI)

Force Protection Quiz Answers
(From Page 14)

Section I: Stuttgart & Garmisch

1. c

6. c

2. b

7. d

3. a-iv, b-ii, c-iii, d-i

8. a

4. a

9. c

5. b

10. F

Section II: United States

1. a

2. a

3. a-iii, b-i, c-ii, d-iv

4. c

5. b

6. d

7. b

8. d

9. F

10. F

Bonus I: Directorate of Plans, Training, Mobilization & Security

Bonus II: Donald Rumsfeld (1975-1977)

Bonus III: The base

Section III: International

1. d

2. a

3. a-i, b-iv, c-iii, d-ii

4. b

5. d

6. c

7. c

8. b

9. c

10. c

Scoring

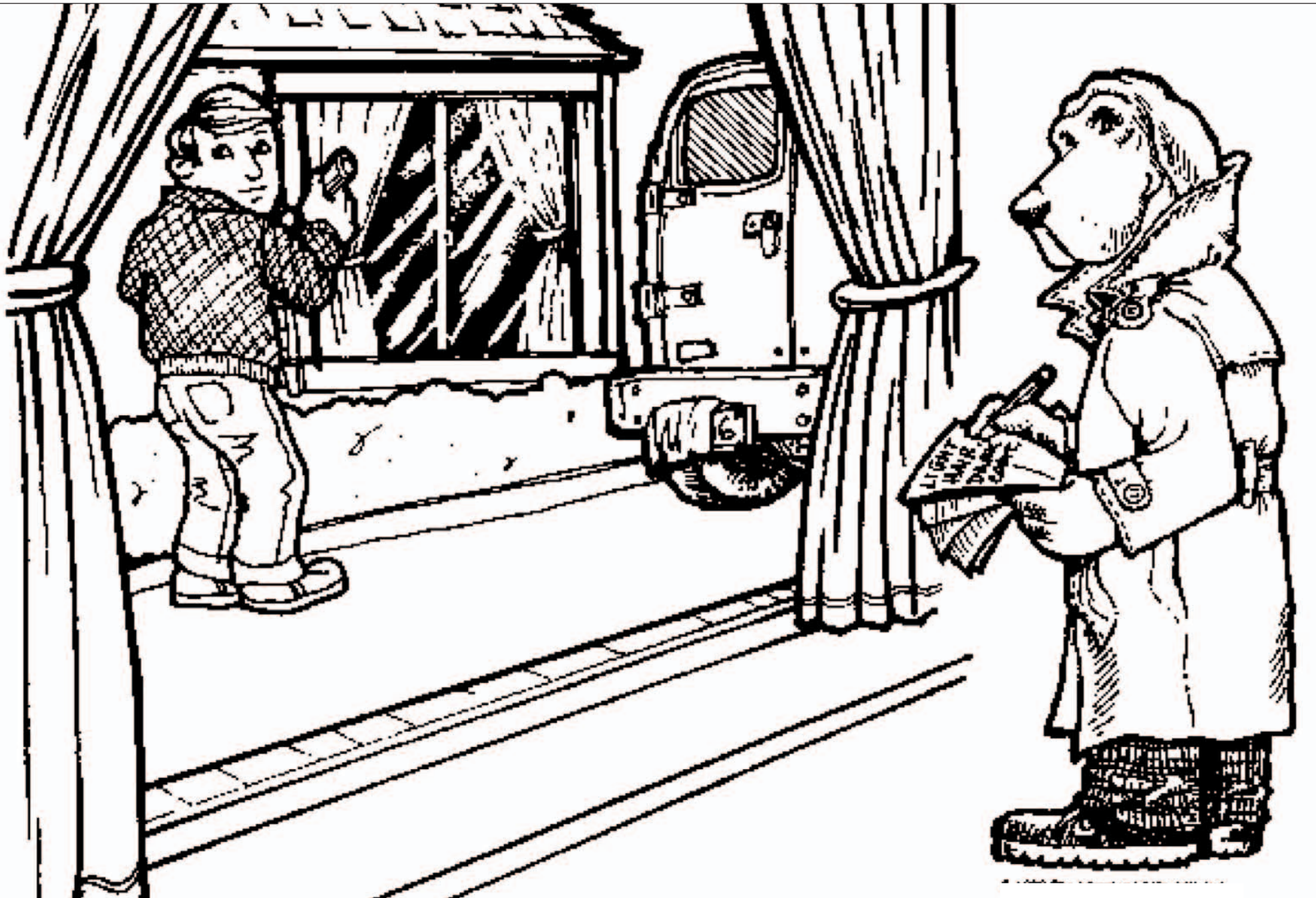
30-33: ★★★★★

27-29: ★★★★

24-26: ★★★

21-23: ★★

18-20: ★



**HEART DISEASE***doesn't***CARE WHAT YOU WEAR****IT'S THE #1 KILLER OF WOMEN**

These women know *The Heart Truth*—no matter how great you look on the outside, heart disease can strike on the inside. And being a woman won't protect you.

Try these risk factors on for size: Do you have high blood pressure? High blood cholesterol? Diabetes? Are you inactive? Are you a smoker? Overweight? If so, this could damage your heart and lead to disability, heart attack, or both.

The Red Dress is a red alert to take heart disease seriously. Talk to your doctor and get answers that may save your life. The Heart Truth is, it's best to know your risks and take action now.

www.hearttruth.gov



*Wear red to the Stuttgart Wellness Center Feb. 3
and receive a free Red Dress Pin.
For details call 430-4073/civ. 0711-680-4073*